Overview of PKI Assessment and Audit Efforts

Federal PKI

Technical Working Group

Noel A. Nazario

October 13, 1999

KPMG

Outline

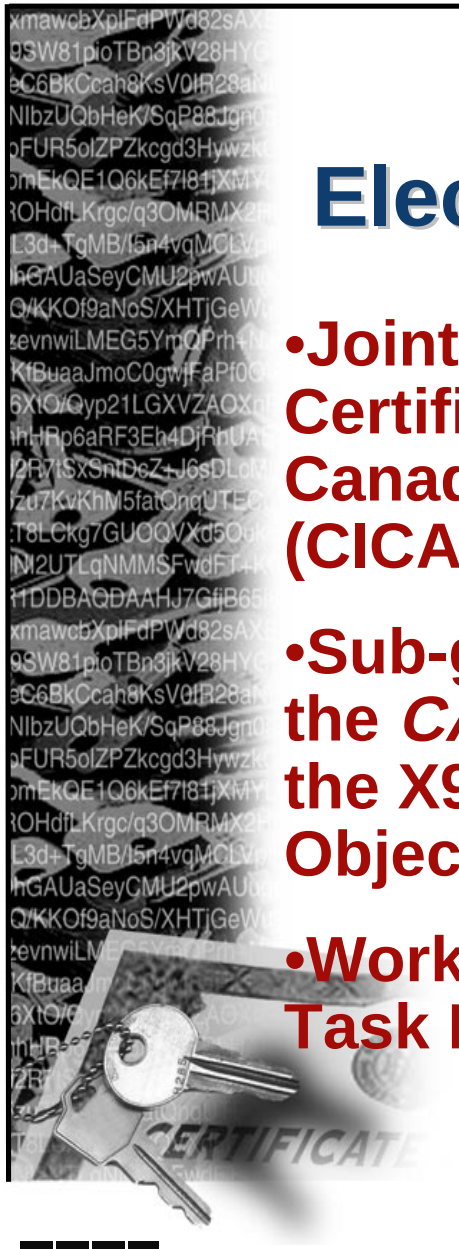
- **Background**
  - **ABA, ISC**
  - **AICPA/CICA**
  - **ANSI/ASC X9F5**
- **PKI Assessment Guideline**
- **CA Trust**
- **ANSI X9.79 standard**

ABA - ISC

- American Bar Association, Information Security Committee
- Previously developed Digital Signature Guidelines
- Currently Developing PKI Assessment Guidelines

American Bar Association Information Security Committee

- **Participants include:**
  - KPMG, IBM, LGS Group
  - VeriSign, Spyrus, CyberTrust, Entrust, and other technology providers
  - McCarter & English, Baker & McKenzie, and other law firms
  - NIST, Government of Canada, and several States
  - West Publishing Company



AICPA/CICA
Electronic Commerce Task Force

- **Joint effort of the of the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA)**
- **Sub-group chaired by KPMG, has developed the *CATrust* principles and criteria based on the X9.79 Certification Authority Control Objectives**
- **Working group will present *CATrust* to the EC Task Force October 14**

KPMG

AICPA/CICA
Electronic Commerce Task Force

- **Participants include:**
  - **Deloitte & Touche (chair)**
  - **KPMG**
  - **Ernst & Young**
  - **PricewaterhouseCoopers**
  - **Arthur Andersen**

ANSI/ASC X9F5 Working Group

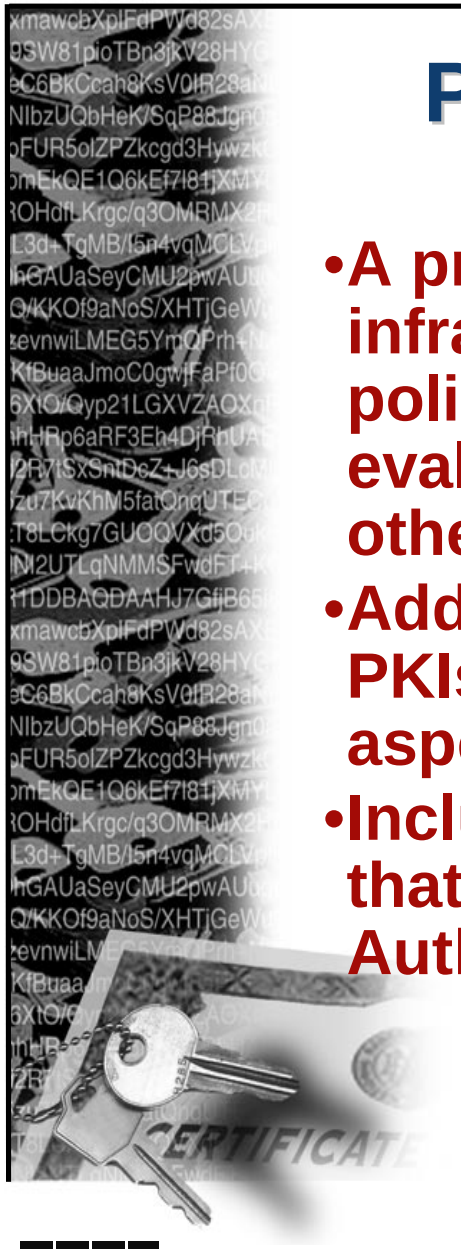
- **ANSI (American National Standards Institute)**
  - **Accredited Standards Committee X9 (Financial Services)**
  - **X9F Subcommittee (Data and Information Security)**
  - **X9F5 (Digital Signature and Certificate Policy Working Group)**
- **Developing the draft ANSI X9.79 standard, *PKI Practices and Policy Framework***
- **Includes PKI/CA audit criteria, and Certificate Authority Control Objectives (CACO)**

KPMG

ANSI X9F5 Working Group

- **Participants include:**
  - E&Y (chair), KPMG, PWC, D&T
  - IBM
  - Federal Reserve Bank
  - First Union, Chase Manhattan, Bank of America
  - American Bankers Association
  - MasterCard, Visa
  - VeriSign, CyberTrust, Spyrus, Baltimore Technologies

PKI Assessment Guidelines



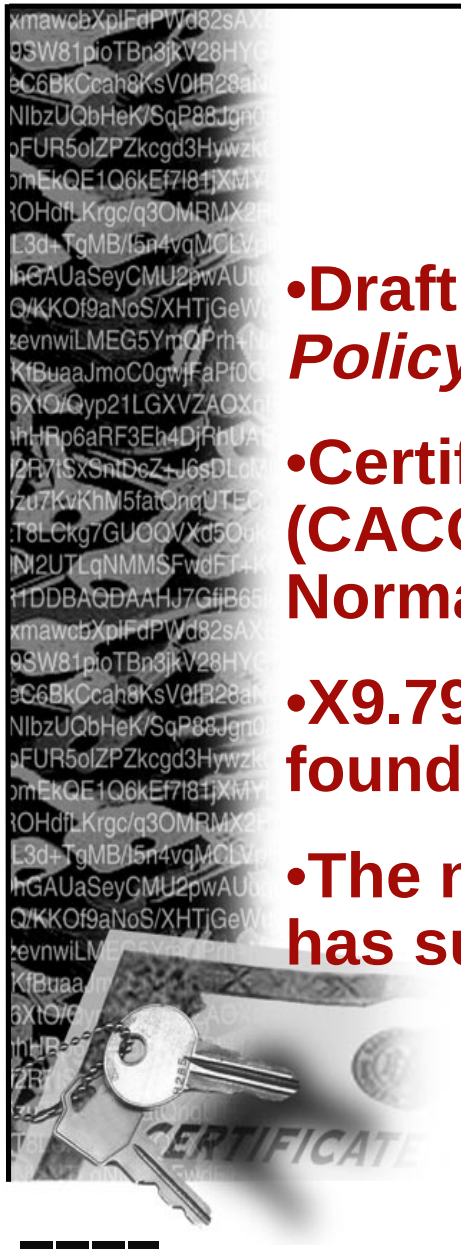
- A process to assure trustworthy public key infrastructure (PKI) by developing certificate policies, and accreditation guidelines for evaluators of certification authorities and other PKI components
- Addresses both technical legal issues of PKIs, but focuses more heavily on the legal aspects
- Includes general PKI/CA audit requirements that reference the X9.79 Certification Authority Control Objectives

CA Trust

- **CA trust was originally targeted to the financial services industry but is applicable to all industries using CAs.**
- **Uses each of the 28 Certification Authority Control Objectives from X9.79.**
- **Detailed X9.79 control objectives are presented as "illustrative controls" that a CA should have in place to meet the control objective. Alternative approaches may used to fulfill the objectives.**

X9.79 Standard

- **Draft ANSI X9.79 standard, *PKI Practices and Policy Framework* (Mark Lundin, *Editor*)**
- **Certificate Authority Control Objectives (CACO) are included in the standard as a Normative Annex**
- **X9.79 will be submitted to ISO TC 68 as the foundation for a new IS.**
- **The new ISO WG will be chaired by US and has support from UK, Canada, and Sweden**

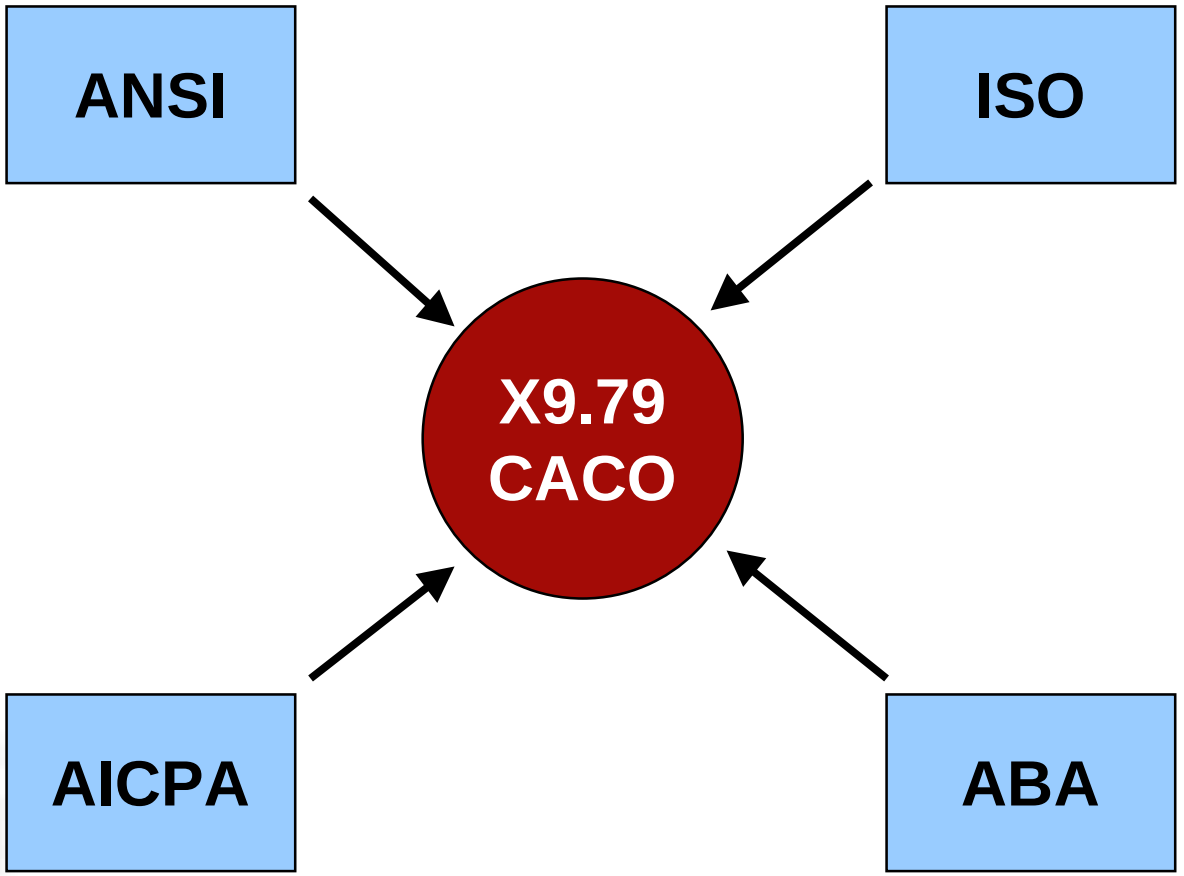


KPMG

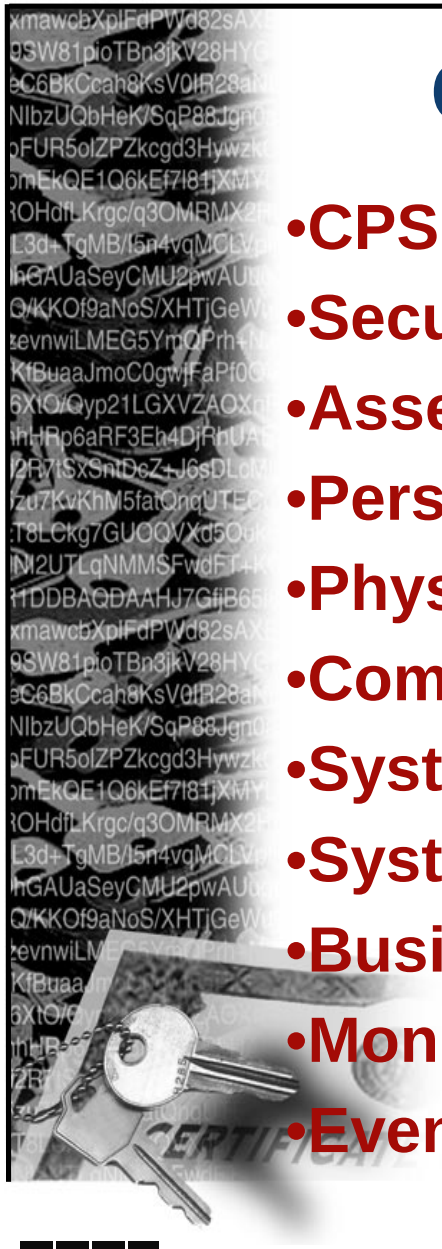
Certificate Management Control Objectives

- **Based on existing standards:**
  - **ANSI X9.57, ISO 15782-1, FIPS 140-1, BS 7799, IETF PKIX-4, NACHA CARAT, and ABA PAG**
- **Primary CA Controls**
- **Key Management Controls**
- **Certificate Life Cycle Controls**

X9.79 CA Control Objectives



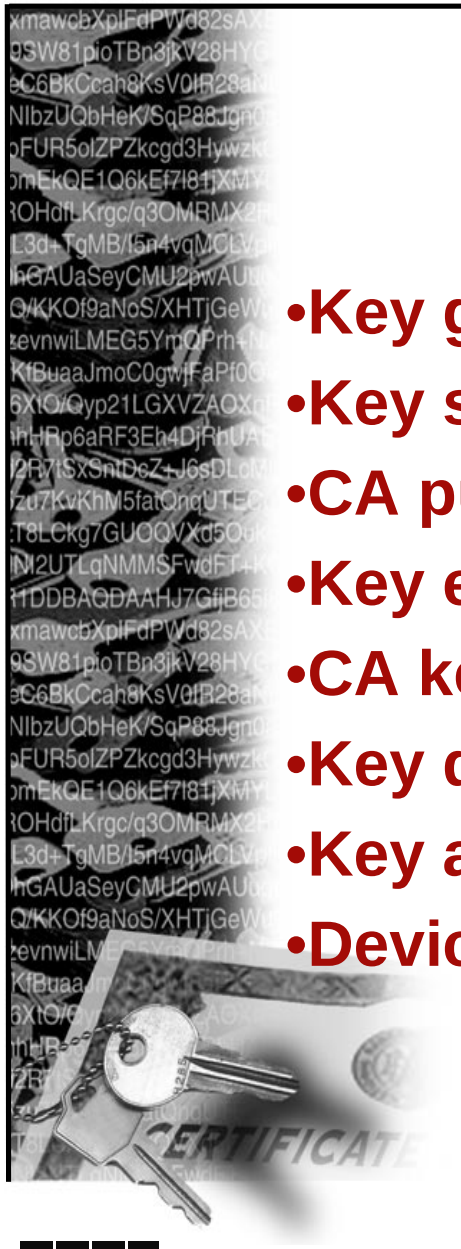
CA Environmental Controls



- CPS and CP management
- Security management
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- System access management
- Systems development and maintenance
- Business continuity management
- Monitoring and compliance
- Event journaling

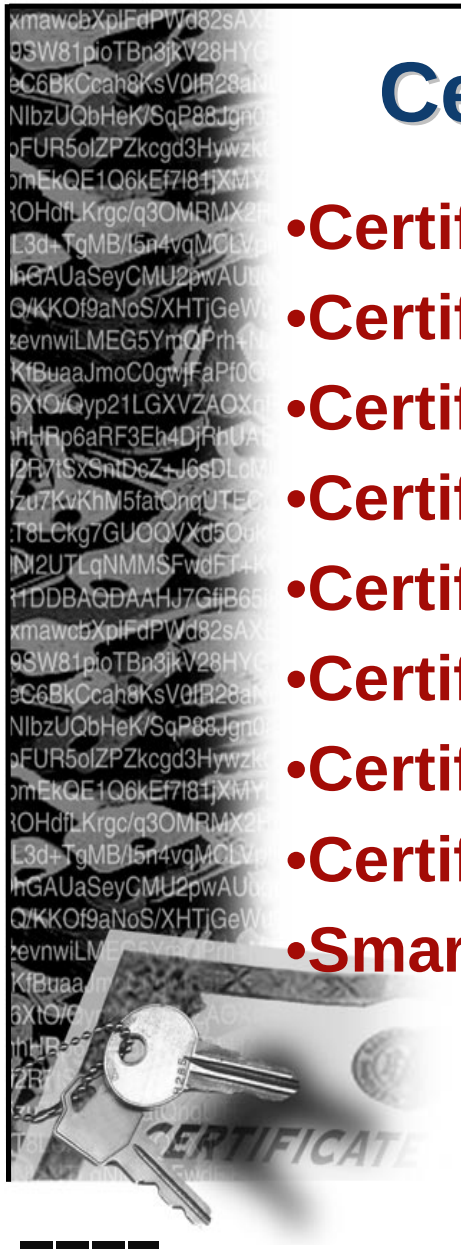
Key Management Life Cycle Controls

- Key generation
- Key storage, backup and recovery
- CA public key distribution
- Key escrow (optional)
- CA key usage
- Key destruction
- Key archival
- Device life cycle management



Certificate Life Cycle Controls

- Certificate registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension (optional)
- Certificate revocation list processing
- Smart card life cycle management (optional)



Questions